CCTV: DEVELOPING PRIVACY BEST PRACTICES

DECEMBER 17 and 18, 2007 – *Day One*

Hilton Arlington

950 North Stafford Street, Arlington, Virginia

Homeland Security

The Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528
t: 703-235-0780; f: 703-235-0442
privacy@dhs.gov; www.dhs.gov/privacy

Technology Perspectives

Issues & Challenges

Jennifer King
Research Specialist
Samuelson Law, Technology and Public Policy Clinic,
University of California-Berkeley School of Law

Homeland Security

Video Surveillance: Issues & Challenges from the Information Management and Usability Perspective

Jennifer King
Samuelson Law, Technology, and Public Policy Clinic
UC Berkeley School of Law

Overview of Discussion

- Information overload
- Information management & retrieval
- Personnel and expertise
- “Forensic” vs. Live Monitored Systems

- A few notes:
- Won’t be covering privacy issues in this discussion
- Resource efficiency:
  - How effectively and efficiently does VS allow police organizations to deploy their resources? Do the benefits outweigh more cops on the street?
  - How effective is VS at fighting crime?

Information overload?

- How will you manage the amount of data VS gives you? Such as . . .
- Understanding context:
  - Discerning what's relevant & what's noise
  - What are true safety threats vs. overreaching
  - How to avoid issues of bias, racial profiling, etc.
- Coordinating information flows from VS feeds and other info gathering sources (dispatch, patrols, etc.)
- Routing of VS feeds into patrol cars
  - Multitasking?
  - How safe?
  - How effective?

Information management & retrieval

- Issues to be aware of:
- Long term storage and archive management
  - How will you organize/index/search?
  - How will you manage 1000s of cases?
- Video search
  - How will you isolate critical segments?
  - Timestamps/tagging/annotating
- Your archive management strategy may effect:
  - Oversight
  - Auditing & effectiveness
  - Workflows

Personnel and expertise

- Who is going to manage your system?
  - Many medium to small jurisdictions use staff officers with no expertise in the area
- Who is going to provide IT support?
  - All enterprise software requires “care and feeding” to maintain after installation, such as system upgrades, patches, ongoing training, etc.
  - If you have no qualified in-house support, you may need to sign a service contract with a vendor
- Who will train your investigators?
  - Investigators need to understand how to use the technical system, as well as any additional skills needed to interpret evidence
- How will you know if your system works?
  - How will you track effectiveness, both in terms of public safety and as a useful tool/resource?

“Forensic” system or live monitoring?

- Forensic:
  - Usually fixed installation, no live monitoring
  - What is captured is largely accidental
  - What effect will this have?
    - Displace crime?
    - If no direct relationship between action and recording, will it have any deterrent effect?
- Live monitored:
  - Human operators using PTZ cameras to actively monitor an area
  - Presumably resources would be deployed as a result of what operators observe
  - Issues (on next slide)
  - What effect will this have?
    - Will it deter or displace?

Issues with Live Monitored Systems

- Monitoring is an active activity: requires focus and stamina
  - Research suggests limits of attention at between 30m to 2hrs
- Visual attention:
  - How many screens can one person focus on effectively?
  - What is the optimal ratio of live feeds to one person?
- Info overload: managing info coming in from multiple sources (dispatch, officers, etc.)
- Qualifications and training:
  - Should police officers perform this job? Dispatchers? Others?
  - How extensive of training is required?
    - How to use the software/system
    - How to use video as an effective method for public safety
    - How to avoid issues of bias and racial profiling